Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template EB Docket 06-36

Date filed:	02/15/2013
Name of company covere by this certification:	Momentum Telecom 2700 Corporate Drive Suite 200 Birmingham, AL 35242
Form 499 Filer ID:	821474
Name of signatory:	Charles E. Richardson III
Title of signatory:	Vice President & Secretary

I, Charles E. Richardson III, certify that I am an officer of the company named Momentum Telecom, Inc, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.
See 47 C.F.R. § 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of
CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17,which requires truthful and accurate statements to the Commission. The company also acknowledges that
false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____

1 Attachment

Attachment 1

Annual 47 **C.F.R. § 64.2009(e) CPNI Certification**

EB Docket 06-36

Momentum Telecom, Inc.
2700 Corporate Drive Suite 200
Birmingham, AL 35242

Momentum Telecom, Inc. (the Company) is a competitive local exchange carrier (CLEC) with retail telephone customers (customers) in nine southern states.[1] The Company has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. For example, the Company authenticates customers without the use of readily available biographical information (such as customer's social security number, or the last four digits of that number, the customer's mother's maiden name, a home address, or a date of birth), or account information, prior to (i) allowing the customer online access to CPNI related to a telecommunications service account or (ii) verbally communicating CPNI to the customer. Specifically, the Company authenticates its customer through a password previously mailed to the customer's address of record with the Company

Company may negotiate alternative authentication procedures for services that Company provides to business customers that have both a dedicated account representative and a contract that specifically addresses Company's protection of CPNI.

Company trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out Company's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

The Company notifies customers promptly by mail whenever a password, customer response to a backup means of authentication for lost or stolen passwords, online account, or address of record is created or changed. This notification is not provided when the customer initiates service, including the selection of a password at service initiation.

The Company does not share CPNI with third parties for purposes of marketing products or services. The Company does not use CPNI for marketing purposes.

Company discloses and permits access to CPNI where required by law (e.g., under a lawfully issued subpoena).

The Company will report CPNI breaches electronically within 7 days to the US Secret Service and the FBI

[1] NC, SC, GA, FL, KY, TN, AL, MS, LA.

through the designated central reporting facility at https://www.cpnireporting.gov. Following electronic notification to the designated central reporting facility, the affected customer will be promptly notified by mail unless the Company is otherwise instructed by law enforcement..

The Company protects its stored CPNI records via a password protected, secured web site.